(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－351565
（P2002－351565A）
(43)公開日　平成14年12月６日(2002.12.6)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　1/00		Ｇ０６Ｆ　15/00	３３０Ａ	５Ｂ０５８
15/00	３３０	Ｇ０６Ｋ　17/00	Ｓ	５Ｂ０７６
Ｇ０６Ｋ　17/00		Ｇ０６Ｆ　9/06	６６０Ｆ	５Ｂ０８５

審査請求　未請求　請求項の数12　ＯＬ　（全 14 頁）

(21)出願番号　特願2001－153700(P2001－153700)

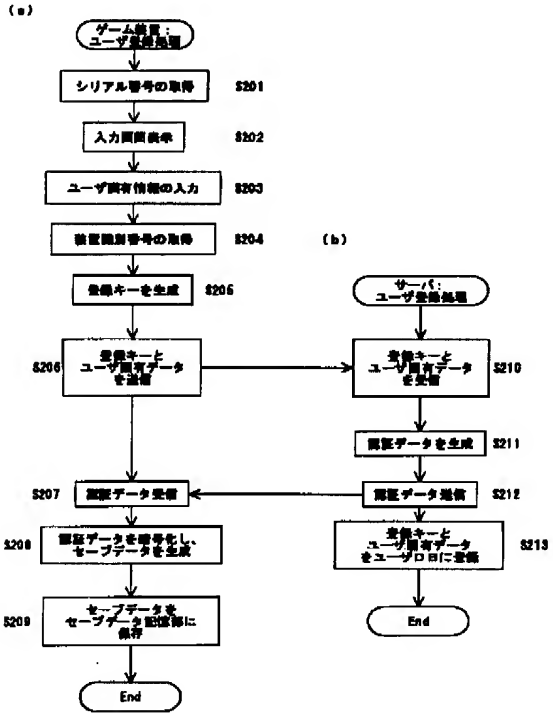
(22)出願日　平成13年５月23日(2001.5.23)

(71)出願人　500086087
株式会社インターステイト
東京都渋谷区渋谷三丁目11番２号
(72)発明者　金子　浩
東京都渋谷区渋谷三丁目11番２号　株式会社インターステイト内
(74)代理人　100092082
弁理士　佐藤　正年　（外１名）

Ｆターム(参考)　5B058 CA27 KA31 YA20
5B076 FB06
5B085 AE13 AE23 BG07

(54)【発明の名称】　不正使用防止システム、不正使用防止方法及び不正使用防止プログラム

(57)【要約】　（修正有）
【課題】　プログラム記録媒体の不正コピーによる不正使用やデータの改竄による不正使用を防止する。
【解決手段】　クライアントコンピュータでは、ユーザ固有データの入力しＳ２０２，Ｓ２０３、プログラム記録媒体に固有のシリアル番号とクライアントコンピュータに固有の装置識別データを取得しＳ２０１，Ｓ２０４、シリアル番号と装置識別データとに基づいて登録キーを生成しＳ２０５、登録キーとユーザ固有データをサーバコンピュータに送信するＳ２０６。サーバコンピュータでは、登録キーとユーザ固有データを受信しＳ２１０、登録キーに基づいて認証データを生成しＳ２１１、クライアントコンピュータに送信するＳ２１２。クライアントコンピュータでは、認証データを受信しＳ２０７、セーブデータを生成するＳ２０８。実行時に、セーブデータと識別データとに基づいてプログラムを起動するか否かを判断する。



【特許請求の範囲】

【請求項１】　サーバコンピュータと、プログラムを実行する複数のクライアントコンピュータとからなる不正使用防止システムにおいて、

前記サーバコンピュータは、

予めプログラム記録媒体に固有のシリアル番号を記録したデータベースと、

各クライアントコンピュータから、前記シリアル番号とクライアントコンピュータに固有の装置識別データとに基づいた登録キーと、ユーザ固有データとを受信するクライアントデータ受信手段と、

ユーザ認証のための認証データを、前記登録キーに基づいて生成する認証データ生成手段と、

前記認証データをクライアントコンピュータに送信する認証データ送信手段と、

前記登録キーと前記ユーザ固有データとを、前記シリアル番号と対応づけて前記データベースに記録する登録手段と、を備えたものであり、

前記クライアントコンピュータは、

クライアントコンピュータに固有の装置識別データを予め記憶した識別データ記憶手段と、

ユーザ固有データを入力させる入力処理手段と、

前記シリアル番号と前記装置識別データとに基づいて登録キーを生成する登録キー生成手段と、

前記登録キーとユーザ固有データとを、前記サーバコンピュータに送信するクライアントデータ送信手段と、

前記サーバコンピュータから前記認証データを受信する認証データ受信手段と、

受信した認証データに基づいてセーブデータを生成するセーブデータ生成手段と、

前記生成されたセーブデータを記憶するセーブデータ記憶手段と、

プログラム実行時に、前記セーブデータ記憶手段に記録されたセーブデータと前記装置識別データとに基づいてプログラムを起動するか否かを判断する認証手段と、を備えたものであることを特徴とする不正使用防止システム。

【請求項２】　前記サーバコンピュータの認証データ生成手段は、前記認証データを、前記登録キーと前記ユーザ固有データとに基づいて生成するものであり、

前記クライアントコンピュータの認証データ受信手段は、サーバコンピュータから前記認証データを受信するものであり、

前記クライアントコンピュータの認証手段は、プログラム実行時に、前記セーブデータ記憶手段に記録されたセーブデータと、前記装置識別データ及び／又は前記ユーザ固有データとに基づいてプログラムを起動するか否かを判断するものであることを特徴とする請求項１に記載の不正使用防止システム。

【請求項３】　予めプログラム記録媒体に固有のシリアル番号を記録したデータベースと、

各クライアントコンピュータから、前記シリアル番号とクライアントコンピュータに固有の装置識別データとに基づいた登録キーと、ユーザ固有データとを受信するクライアントデータ受信手段と、

ユーザ認証のための認証データを、前記登録キーに基づいて生成する認証データ生成手段と、

前記認証データをクライアントコンピュータに送信する認証データ送信手段と、

前記登録キーと前記ユーザ固有データとを、前記シリアル番号に対応づけて前記データベースに記録する登録手段と、を備えたことを特徴とする不正使用防止サーバ。

【請求項４】　前記認証データ生成手段は、前記認証データを、前記登録キーと前記ユーザ固有データとに基づいて生成するものであることを特徴とする請求項３に記載の不正使用防止サーバ。

【請求項５】　装置固有の装置識別データを予め記憶する識別データ記憶手段と、

ユーザ固有データを入力させる入力処理手段と、

プログラム記録媒体に固有のシリアル番号と装置固有の装置識別データとに基づいて、登録キーを生成する登録キー生成手段と、

前記登録キーとユーザ固有データとを、サーバコンピュータに送信するクライアントデータ送信手段と、

サーバコンピュータから前記登録キーに基づいて生成された認証データを受信する認証データ受信手段と、

前記受信した認証データに基づいてセーブデータを生成するセーブデータ生成手段と、

前記セーブデータを格納するセーブデータ記憶手段と、

プログラム実行時に、前記セーブデータ記憶手段に記録されたセーブデータと前記装置識別データとに基づいてプログラムを起動するか否かを判断する認証手段と、を備えたことを特徴とする不正使用防止装置。

【請求項６】　前記認証データ受信手段は、サーバコンピュータから前記登録キーと前記ユーザ固有データとに基づいて生成された認証データを受信するものであり、

前記認証手段は、プログラム実行時に、前記セーブデータ記憶手段に記録されたセーブデータと、前記装置識別データ及び／又は前記ユーザ固有データとに基づいてプログラムを起動するか否かを判断するものであることを特徴とする請求項５に記載の不正使用防止装置。

【請求項７】　プログラムのユーザを管理するサーバコンピュータと、プログラムを実行する複数のクライアントコンピュータとの間でデータを送受信することにより、クライアントコンピュータで実行するプログラムの不正使用を防止する不正使用防止方法において、

クライアントコンピュータでは、

ユーザ固有データの入力を促す入力処理ステップと、プログラム記録媒体に固有のシリアル番号とクライアントコンピュータに固有の装置識別データとに基づいて登録

キーを生成する登録キー生成ステップと、前記登録キーとユーザ固有データをサーバコンピュータに送信するクライアントデータ送信ステップと、を含み、
サーバコンピュータでは、
クライアントコンピュータから受信した前記登録キーに基づいて認証データを生成する認証データ生成ステップと、前記認証データをクライアントコンピュータに送信する認証データ送信ステップと、予めシリアル番号を記録したデータベースに、前記登録キーと前記ユーザ固有データを前記シリアル番号と対応づけて記録する登録ステップと、を含み、
前記認証データを受信したクライアントコンピュータでは、
前記認証データに基づいてセーブデータを生成し、生成されたセーブデータをセーブデータ記憶手段に記録するセーブデータ生成ステップと、プログラムの実行時に、前記セーブデータ記憶手段に記憶されたセーブデータと前記識別データとに基づいてプログラムを起動するか否かを判断する認証ステップと、を含むことを特徴とする不正使用防止方法。

【請求項８】　サーバコンピュータ側で、
各クライアントコンピュータから、プログラム記録媒体に固有のシリアル番号とクライアントコンピュータに固有の装置識別データとに基づいた登録キーと、ユーザ固有データとを受信するクライアントデータ受信ステップと、
ユーザ認証のための認証データを、前記登録キーに基づいて生成する認証データ生成ステップと、
前記認証データをクライアントコンピュータに送信する認証データ送信ステップと、
前記登録キーと前記ユーザ固有データとを、前記シリアル番号に対応づけてデータベースに記録する登録ステップと、を含むことを特徴とする不正使用防止方法。

【請求項９】　前記認証データ生成ステップは、前記認証データを、前記登録キーと前記ユーザ固有データとに基づいて生成するものであることを特徴とする請求項８に記載の不正使用防止方法。

【請求項１０】　クライアントコンピュータ側で、
ユーザ固有データを入力させる入力処理ステップと、
プログラム記録媒体に固有のシリアル番号と装置固有の装置識別データとに基づいて、登録キーを生成する登録キー生成ステップと、
前記登録キーとユーザ固有データとを、サーバコンピュータに送信するクライアントデータ送信ステップと、
サーバコンピュータから前記登録キーに基づいて生成された認証データを受信する認証データ受信ステップと、
前記認証データに基づいてセーブデータを生成し、生成されたセーブデータをセーブデータ記憶手段に記録するセーブデータ生成ステップと、
プログラムの実行時に、前記セーブデータ記憶手段に記憶されたセーブデータと前記識別データとに基づいてプログラムを起動するか否かを判断する認証ステップと、
を含むことを特徴とする不正使用防止方法。

【請求項１１】　前記認証データ受信ステップは、サーバコンピュータから前記登録キーと前記ユーザ固有データとに基づいて生成された認証データを受信するものであり、
前記認証ステップは、プログラム実行時に、前記セーブデータ記憶手段に記録されたセーブデータと、前記装置識別データ及び／又は前記ユーザ固有データとに基づいてプログラムを起動するか否かを判断するものであることを特徴とする請求項１０に記載の不正使用防止方法。

【請求項１２】　請求項７～１１のいずれか１項に記載の不正使用防止方法をコンピュータに実行させるための不正使用防止プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ゲーム装置などのコンピュータで実行するゲームプログラムあるいは任意のプログラムを購入したユーザ以外の前記プログラムの不正な使用又は使用するコンピュータ以外での前記プログラムの不正な使用を防止する不正使用防止システム、不正使用防止装置及び不正使用防止方法に関するものであり、特にユーザ情報やプログラム記録媒体のシリアル番号を管理するサーバコンピュータと連携して不正使用を防止する不正使用防止システム、不正使用防止装置及び不正使用防止方法に関する。

【０００２】

【従来の技術】ゲームプログラム等のソフトウェアは、主としてＣＤ、ＤＶＤ、フロッピー（登録商標）ディスク（ＦＤ）、フラッシュメモリ等のメモリカード等の記録媒体に記録してユーザに販売しているが、正当に購入されたソフトウェアを他の記録媒体に不正コピーして、不正コピーされたソフトウェアを正当に購入したユーザ以外の不正ユーザが使用したり、他のコンピュータやゲーム装置で使用するという不正使用が近年問題となっている。

【０００３】このため、ゲームプログラム等のソフトウェアを製造販売するソフトウェアメーカや、ゲーム装置等のコンピュータを製造販売するハードウェアメーカでは、このような不正コピーを防止する手段として種種の方策を講じている。このような不正コピー防止手段としては、ソフトウェア側でコピープロテクトを行うソフトウェアプロテクトとゲーム装置等のハードウェア側でコピープロテクトを行うハードウェアプロテクトの２つの方法がある。

【０００４】ソフトウェアプロテクト手段として、第１の手段は殆ど全てのソフトウェアの商品について使用されているものであり、工場でソフトウェア記録媒体を量産する段階で予めコンピュータ上のファイルシステムで

認識不可能な非コピー属性の識別データを記録媒体に記録しておき、ユーザ側でのプログラム実行時にこの識別データの有無をチェックし、正規の記録媒体に記録されたプログラムから起動されたものか（正規の製品か）、不正コピーされた記録媒体のプログラムから起動されたものかを判断するものである。そして、正規の記録媒体である場合にのみプログラムを実行を継続するようにして不正コピーされた記録媒体のプログラムの実行を不可能にする事により実質的にプログラムの不正コピーを無効にすることによって、ソフトウェア製品の不正コピーを防止している。

【０００５】また、第２のソフトウェアプロテクト手段は、ソフトウェアメーカで講じる主流のプロテクト手段であり、記録媒体に記録したプログラム中に、予めユーザ認証のためのフェイズ又はプログラムを組み込んでおく。そして、ソフトウェア起動後にユーザ認証フェイズ又はプログラムを実行してソフトウェアパッケージに含まれるシリアル番号やプログラム等に基づいて、正規の製品か、不正コピーされた製品かをチェックし、正規の記録媒体である場合にのみプログラムを実行を継続するようにして不正コピーされた記録媒体のプログラムの実行を不可能として実質的にプログラムの不正コピーを無効にするものである。このプロテクト手段におけるユーザ認証のプログラムとしては種種のものが開発されている。

【０００６】一方、ハードウェアプロテクト手段としては、ゲーム装置やコンピュータ等のハードウェアの各種ポートに接続する専用部品を設け、プログラム側で対象ポートからの信号を受信して、受信信号が異常である場合には不正コピーされた製品であると判断するものである。

【０００７】

【発明が解決しようとする課題】しかしながら、このような従来の不正使用防止手段には次のような問題点がある。第１のソフトウェアプロテクト手段では、記録媒体に非コピー属性の識別データを記録しているため、ファイルシステム上はこの識別データを認識することはできないが、近年流通しているＣＤ－Ｒ、ＣＤ－ＲＷ、ＤＶＤ－ＲＡＭ等には媒体ごとセクタ単位で複製することは可能である。この場合、識別データも同時に複製されてしまうため、プログラム側で正規のソフトウェア製品か、不正コピーされたソフトウェアかを判別することができないという問題がある。

【０００８】また、第２のソフトウェアプロテクト手段では、記録媒体中のプログラムでチェックするシリアル番号を変更する等のデータ改竄が行えたり、あるいはＣＤ－Ｒ等の記録媒体に複製したあと、シリアル番号登録を行うこともできてしまい、容易にソフトウェアプロテクトを解除することが可能となるという問題がある。

【０００９】更に、従来のハードウェアプロテクト手段では、パッケージに専用部品を同梱して販売しなければならず、製品の製造コストが増大する。また、対象ポートからの受信信号を解析するプログラムを改竄することも可能である。

【００１０】一方、ソフトウェアに有効期限を設定し、有効期限経過後はそのプログラムを実行することができないような方法も考えられるが、これでは、販売期間が制限されてしまい、開発に要した投資を十分に回収できない。

【００１１】本発明はこのような問題点に鑑みてなされたものであり、記録媒体の不正コピーによる不正使用や、データの改竄によるプログラムの不正使用を防止することができる不正使用防止方法及び不正使用防止システムを提供することを主な目的とする。本発明の別の目的は低コストでソフトウェアの不正使用を防止することができる不正使用防止方法及び不正使用防止システムを提供することである。

【００１２】

【課題を解決するための手段】上述の目的を達成するため、請求項１に係る発明は、サーバコンピュータと、プログラムを実行する複数のクライアントコンピュータとからなる不正使用防止システムにおいて、前記サーバコンピュータは、予めプログラム記録媒体に固有のシリアル番号を記録したデータベースと、各クライアントコンピュータから、前記シリアル番号とクライアントコンピュータに固有の装置識別データとに基づいた登録キーと、ユーザ固有データとを受信するクライアントデータ受信手段と、ユーザ認証のための認証データを、前記登録キーに基づいて生成する認証データ生成手段と、前記認証データをクライアントコンピュータに送信する認証データ送信手段と、前記登録キーと前記ユーザ固有データとを、前記シリアル番号と対応づけて前記データベースに記録する登録手段と、を備えたものであり、前記クライアントコンピュータは、クライアントコンピュータに固有の装置識別データを予め記憶した識別データ記憶手段と、ユーザ固有データを入力させる入力処理手段と、前記シリアル番号と前記装置識別データとに基づいて登録キーを生成する登録キー生成手段と、前記登録キーとユーザ固有データとを、前記サーバコンピュータに送信するクライアントデータ送信手段と、前記サーバコンピュータから前記認証データを受信する認証データ受信手段と、受信した認証データに基づいてセーブデータを生成するセーブデータ生成手段と、前記生成されたセーブデータを記憶するセーブデータ記憶手段と、プログラム実行時に、前記セーブデータ記憶手段に記録されたセーブデータと前記装置識別データとに基づいてプログラムを起動するか否かを判断する認証手段と、を備えたものであることを特徴とする。

【００１３】本発明では、ユーザのプログラム使用開始時に、シリアル番号と装置識別データに基づいた登録キ

ーを生成して、ユーザ固有情報と共にサーバコンピュータへ送信する。ここで、「シリアル番号と装置識別データに基づいて登録キーを生成する」とは、少なくともシリアル番号と装置識別データを含むように登録キーを生成することをいい、他のデータを含めて登録キーを生成するように構成しても良い。また、シリアル番号と装置識別データとを暗号化して登録キーに含めるように構成してもよい。

【００１４】このように、登録キーにはシリアル番号が含められており、サーバコンピュータ側ではこの認証データに含まれるシリアル番号と受信したユーザ固有データとを対応付けてデータベースに記録する。このため、一つのソフトウェアに対して使用可能なユーザを確定して制限することができる。

【００１５】また、本発明では、サーバコンピュータ側で、クライアントコンピュータから受信した登録キーに基づいて認証データを生成してユーザに送信する。一方、クライアントコンピュータ側では、受信した認証データに基づいてセーブデータを生成してセーブデータ記憶手段に格納する。ここで、「登録キーに基づいて認証データを生成する」とは、少なくとも登録キーを含むように認証データを生成することをいい、ユーザ固有データ等の他のデータを含めて認証データを生成するように構成しても良い。また、登録キーを暗号化して認証データに含めるように構成してもよい。また、「認証データに基づいてセーブデータを生成する」とは、少なくとも認証データを含むようにセーブデータを生成することをいい、他のデータを含めてセーブデータを生成するように構成しても良い。また、認証データを暗号化してセーブデータに含めるように構成してもよい。

【００１６】このように、セーブデータには認証データが含まれ、認証データには登録キーが含まれており、更に登録キーにはシリアル番号と装置識別番号が含まれるので、結果としてセーブデータにはシリアル番号と装置識別番号が含まれることになる。そして、クライアントコンピュータでは、プログラム実行時にこのセーブデータに基づいてプログラムを起動すべきか否かを判断しているので、記録媒体のプログラムを、最初にプログラムを起動したクライアントコンピュータ以外の装置で実行することができなくなり、プログラムを複数の装置で使用するという不正使用を防止することができる。

【００１７】また、本発明では、記録媒体を不正コピーした場合でも、セーブデータ記憶手段に格納されたセーブデータがわからなければ、プログラムを起動できないので、記録媒体の不正コピーが実質的に無効となり、不正コピーの抑止を図ることができる。

【００１８】更に、本発明ではシリアル番号と装置識別番号からセーブデータを単純に生成しているのではなく、シリアル番号と装置識別番号から登録キーの生成、登録キーから認証データの生成、及び認証データからセーブデータへの生成という、クライアントコンピュータとサーバコンピュータの双方で、データの加工を複数回行うことによりセーブデータを生成している。このため、セーブデータからシリアル番号や装置識別番号を解析したり、改竄することは非常に困難となり、データ改竄によるプログラムの不正使用を防止することができる。

【００１９】加えて、本発明ではハードウェアとしてはセーブデータ記憶手段にセーブデータを格納するだけで不正使用を防止することができるので、従来のハードウェアプロテクト手段のように不正使用防止のための専用部品を製造したり同梱する必要がなく、製造コストの低減が図られる。

【００２０】本発明で使用するシリアル番号は、プログラム記録媒体に固有のものであればよい。例えば、シリアル番号をプログラム記録媒体の所定の記憶領域に予め記録した形式でソフトウェアパッケージを出荷する場合には、この記録媒体に記録されたシリアル番号を用いることができる。この場合には、登録キー生成手段を、プログラム記録媒体の前記記憶領域からシリアル番号を読み出して、当該読み出したシリアル番号と装置識別データとから登録キーを生成するように構成すれば良い。

【００２１】また、シリアル番号を記録媒体自体には格納せずに、記録媒体の添付シート等に固有のシリアル番号を記述した形式でソフトウェアパッケージを出荷する場合には、この添付シート等に記述されたシリアル番号を用いても良い。この場合には、添付シートに記述されたシリアル番号をユーザに入力させるために、入力処理手段を、ユーザ固有データの他、シリアル番号の入力も促すように構成し、更に登録キー生成手段を、入力されたシリアル番号と装置識別データとから登録キーを生成するように構成すれば良い。

【００２２】本発明における認証手段は、プログラム実行時に、セーブデータと、装置識別データとに基づいてプログラムを起動するか否かを判断するものであればよく、記録媒体にシリアル番号が記録されている場合には、更にセーブデータと記録媒体から読み出したシリアル番号とを比較するように構成することもできる。この場合には、同一シリアル番号に基づくセーブデータを保存した装置以外の装置ではプログラムを実行することができなくなるので、プログラムを複数の装置で使用するという不正使用を防止することができる。

【００２３】請求項２に係る発明は、請求項１に記載の不正使用防止システムにおいて、前記サーバコンピュータの認証データ生成手段は、前記認証データを、前記登録キーと前記ユーザ固有データとに基づいて生成するものであり、前記クライアントコンピュータの認証データ受信手段は、サーバコンピュータから前記認証データを受信するものであり、前記クライアントコンピュータの認証手段は、プログラム実行時に、前記セーブデータ記

憶手段に記録されたセーブデータと、前記装置識別データ及び／又は前記ユーザ固有データとに基づいてプログラムを起動するか否かを判断するものであることを特徴とする。

【００２４】本発明では、認証データを更にユーザ固有データに基づいて生成しているので、クライアント側で生成されるセーブデータは、結果としてシリアル番号と装置識別番号の他、ユーザ固有データにも基づいたものとなる。そして、クライアント側の認証手段では、プログラム実行時にこのセーブデータと、前記装置識別データ及び／又はユーザ固有データとに基づいてプログラムを起動するか否かを判断するので、不正ユーザの正規ユーザのなりすましによるプログラムの不正使用を防止することができる。

【００２５】本発明における認証手段は、プログラム実行時に、セーブデータと、装置識別データ及び／又はユーザ固有データとに基づいてプログラムを起動するか否かを判断するものであればよく、セーブデータとユーザ固有データとに基づく判断は以下のものがあげられる。例えばプログラム実行時にセーブデータの入力と共に任意のユーザ固有データを入力するように構成すれば、使用開始時にサーバに登録したユーザ以外の使用者か否かを判断することができる。また、このようなプログラム実行時におけるユーザの入力を省略するために、使用開始時にユーザが入力したユーザ固有データをユーザデータ記憶手段等の記憶手段に格納しておき、プログラム実行時に、このユーザデータ記憶手段からユーザ固有データを読み出し、セーブデータから抽出あるいは復号したユーザ固有データと一致するか否か判断するように構成しても良い。

【００２６】請求項３に係る発明は、予めプログラム記録媒体に固有のシリアル番号を記録したデータベースと、各クライアントコンピュータから、前記シリアル番号とクライアントコンピュータに固有の装置識別データとに基づいた登録キーと、ユーザ固有データとを受信するクライアントデータ受信手段と、ユーザ認証のための認証データを、前記登録キーに基づいて生成する認証データ生成手段と、前記認証データをクライアントコンピュータに送信する認証データ送信手段と、前記登録キーと前記ユーザ固有データとを、前記シリアル番号に対応づけて前記データベースに記録する登録手段と、を備えたことを特徴とする不正使用防止サーバに係るものである。

【００２７】本発明は、請求項１に記載の不正使用防止システムにおけるサーバコンピュータに係るものであり、請求項１の発明と同様に、一つのソフトウェアに対して使用可能なユーザを確定して制限することができ、またプログラムを複数の装置で使用するという不正使用を防止、不正コピーの抑止、及びデータ改竄によるプログラムの不正使用の防止が図られる。

【００２８】請求項４に係る発明は、請求項３に記載の不正使用防止サーバにおいて、前記認証データ生成手段は、前記認証データを、前記登録キーと前記ユーザ固有データとに基づいて生成するものであることを特徴とする。

【００２９】本発明は、請求項２に記載の不正使用防止システムにおけるサーバコンピュータに係るものであり、請求項２の発明と同様に、不正ユーザの正規ユーザのなりすましによるプログラムの不正使用を防止することができる。

【００３０】請求項５に係る発明は、装置固有の装置識別データを予め記憶する識別データ記憶手段と、ユーザ固有データを入力させる入力処理手段と、プログラム記録媒体に固有のシリアル番号と装置固有の装置識別データとに基づいて、登録キーを生成する登録キー生成手段と、前記登録キーとユーザ固有データとを、サーバコンピュータに送信するクライアントデータ送信手段と、サーバコンピュータから前記登録キーに基づいて生成された認証データを受信する認証データ受信手段と、前記受信した認証データに基づいてセーブデータを生成するセーブデータ生成手段と、前記セーブデータを格納するセーブデータ記憶手段と、プログラム実行時に、前記セーブデータ記憶手段に記録されたセーブデータと前記装置識別データとに基づいてプログラムを起動するか否かを判断する認証手段と、を備えたことを特徴とする不正使用防止装置に係るものである。

【００３１】本発明は、請求項１に記載の不正使用防止システムにおけるクライアントコンピュータに係るものであり、請求項１の発明と同様に、一つのソフトウェアに対して使用可能なユーザを確定して制限することができ、またプログラムを複数の装置で使用するという不正使用を防止、不正コピーの抑止、及びデータ改竄によるプログラムの不正使用の防止が図られる。また、製造コストの低減が図られる。

【００３２】請求項６に係る発明は、請求項５に記載の不正使用防止装置において、前記認証データ受信手段は、サーバコンピュータから前記登録キーと前記ユーザ固有データとに基づいて生成された認証データを受信するものであり、前記認証手段は、プログラム実行時に、前記セーブデータ記憶手段に記録されたセーブデータと、前記装置識別データ及び／又は前記ユーザ固有データとに基づいてプログラムを起動するか否かを判断するものであることを特徴とする。

【００３３】本発明は、請求項２に記載の不正使用防止システムにおけるクライアントコンピュータに係るものであり、請求項２の発明と同様に、不正ユーザの正規ユーザのなりすましによるプログラムの不正使用を防止することができる。

【００３４】請求項７に係る発明は、プログラムのユーザを管理するサーバコンピュータと、プログラムを実行

する複数のクライアントコンピュータとの間でデータを送受信することにより、クライアントコンピュータで実行するプログラムの不正使用を防止する不正使用防止方法において、クライアントコンピュータでは、ユーザ固有データの入力を促す入力処理ステップと、プログラム記録媒体に固有のシリアル番号とクライアントコンピュータに固有の装置識別データとに基づいて登録キーを生成する登録キー生成ステップと、前記登録キーとユーザ固有データをサーバコンピュータに送信するクライアントデータ送信ステップと、を含み、サーバコンピュータでは、クライアントコンピュータから受信した前記登録キーに基づいて認証データを生成する認証データ生成ステップと、前記認証データをクライアントコンピュータに送信する認証データ送信ステップと、予めシリアル番号を記録したデータベースに、前記登録キーと前記ユーザ固有データを前記シリアル番号と対応づけて記録する登録ステップと、を含み、前記認証データを受信したクライアントコンピュータでは、前記認証データに基づいてセーブデータを生成し、生成されたセーブデータをセーブデータ記憶手段に記録するセーブデータ生成ステップと、プログラムの実行時に、前記セーブデータ記憶手段に記憶されたセーブデータと前記識別データとに基づいてプログラムを起動するか否かを判断する認証ステップと、を含むことを特徴とする。

【００３５】本発明は、請求項１に記載の不正使用防止システムを利用した不正使用防止方法であり、請求項１の発明と同様に、一つのソフトウェアに対して使用可能なユーザを確定して制限することができ、またプログラムを複数の装置で使用するという不正使用を防止、不正コピーの抑止、及びデータ改竄によるプログラムの不正使用の防止が図られる。また、製造コストの低減が図られる。

【００３６】請求項８に係る発明は、サーバコンピュータ側で、各クライアントコンピュータから、プログラム記録媒体に固有のシリアル番号とクライアントコンピュータに固有の装置識別データとに基づいた登録キーと、ユーザ固有データとを受信するクライアントデータ受信ステップと、ユーザ認証のための認証データを、前記登録キーに基づいて生成する認証データ生成ステップと、前記認証データをクライアントコンピュータに送信する認証データ送信ステップと、前記登録キーと前記ユーザ固有データとを、前記シリアル番号に対応づけてデータベースに記録する登録ステップと、を含むことを特徴とする不正使用防止方法に係るものである。

【００３７】本発明は、請求項３に記載の不正使用防止サーバによる不正使用防止方法であり、請求項３の発明と同様に、一つのソフトウェアに対して使用可能なユーザを確定して制限することができ、またプログラムを複数の装置で使用するという不正使用を防止、不正コピーの抑止、及びデータ改竄によるプログラムの不正使用の

防止が図られる。

【００３８】請求項９に係る発明は、請求項８に記載の不正使用防止方法において、前記認証データ生成ステップは、前記認証データを、前記登録キーと前記ユーザ固有データとに基づいて生成するものであることを特徴とする。

【００３９】本発明は、請求項４に記載の不正使用防止サーバによる不正使用防止方法であり、請求項４の発明と同様に、不正ユーザの正規ユーザのなりすましによるプログラムの不正使用を防止することができる。

【００４０】請求項１０に係る発明は、クライアントコンピュータ側で、ユーザ固有データを入力させる入力処理ステップと、プログラム記録媒体に固有のシリアル番号と装置固有の装置識別データとに基づいて、登録キーを生成する登録キー生成ステップと、前記登録キーとユーザ固有データとを、サーバコンピュータに送信するクライアントデータ送信ステップと、サーバコンピュータから前記登録キーに基づいて生成された認証データを受信する認証データ受信ステップと、前記認証データに基づいてセーブデータを生成し、生成されたセーブデータをセーブデータ記憶手段に記録するセーブデータ生成ステップと、プログラムの実行時に、前記セーブデータ記憶手段に記憶されたセーブデータと前記識別データとに基づいてプログラムを起動するか否かを判断する認証ステップと、を含むことを特徴とする不正使用防止方法に係るものである。

【００４１】本発明は、請求項５に記載の不正使用防止装置による不正使用防止方法であり、請求項５の発明と同様に、一つのソフトウェアに対して使用可能なユーザを確定して制限することができ、またプログラムを複数の装置で使用するという不正使用を防止、不正コピーの抑止、及びデータ改竄によるプログラムの不正使用の防止が図られる。また、製造コストの低減が図られる。

【００４２】請求項１１に係る発明は、請求項１０に記載の不正使用防止方法において、前記認証データ受信ステップは、サーバコンピュータから前記登録キーと前記ユーザ固有データとに基づいて生成された認証データを受信するものであり、前記認証ステップは、プログラム実行時に、前記セーブデータ記憶手段に記録されたセーブデータと、前記装置識別データ及び／又は前記ユーザ固有データとに基づいてプログラムを起動するか否かを判断するものであることを特徴とする。

【００４３】本発明は、請求項６に記載の不正使用防止装置による不正使用防止方法であり、請求項６の発明と同様に、不正ユーザの正規ユーザのなりすましによるプログラムの不正使用を防止することができる。

【００４４】請求項１２に係る発明は、請求項７～１１のいずれか１項に記載の不正使用防止方法をコンピュータに実行させるための不正使用防止プログラムに係るものであり、請求項７～１１の発明と同様の作用効果を奏

する。

【００４５】

【発明の実施の形態】以下に添付図面を参照して、本発明に係る不正使用防止システム及び不正使用防止方法の好適な実施の形態を詳細に説明する。本実施形態は、本発明の不正使用防止システムを、ゲームプログラムを実行するゲーム装置と、ゲームプログラムのユーザ管理を行うサーバとからなるゲームシステムに適用したものである。

【００４６】（ゲームシステムの全体構成）図４は、本実施形態のゲームシステムのハードウェア構成を示すブロック図である。図４に示すように、本実施形態のゲームシステムは、ゲームソフトウェアのユーザを管理するサーバコンピュータ（以下、「サーバ」という。）と、当該サーバとインターネットを介して接続される複数のゲーム装置とから構成されている。ここでゲーム装置は、本発明のクライアントコンピュータを構成する。

【００４７】（ゲーム装置のハードウェア構成）図４に示すように、本実施形態のゲーム装置には、制御装置４０１と、記憶装置４０５と、外部記憶装置４０６と、通信装置４０７と、表示装置４０３と、音声出力装置４０２と、入力装置４０４と、識別データ記憶部４０８が接続されている。

【００４８】制御装置４０１は、本実施形態のゲーム装置で実行されるユーザ登録プログラムの動作を制御するＣＰＵ等の演算処理部と、ＲＯＭ等で構成されている。記憶装置４０５はメモリカード等の一般的なＲＡＭで構成される。この記憶装置４０５には、後述するセーブデータを格納するセーブデータ記憶部４０９が設けられている。

【００４９】識別データ記憶部４０８はＲＯＭで構成されており、装置識別番号が格納されている。ここで、装置識別番号とは、ゲーム装置ごとに割り当てられた固有の識別番号であり、本発明の装置識別データを構成する。本実施形態のゲーム装置は、割り当てられた装置識別番号が識別データ記憶部４０８に格納された状態で出荷される。

【００５０】外部記憶装置４０６は、例えば、ＣＤ－ＲＯＭ，ＣＤ－Ｒ／ＲＷ，ＤＶＤ－ＲＯＭ，ＤＶＤ－ＲＡＭ、フロッピーディスク（ＦＤ）、等のゲームプログラムを記録した記録媒体と、各媒体に対応して各媒体へのリード又は／及びライトを制御するＣＤ－ＲＯＭドライブ装置，ＣＤ－Ｒ／ＲＷドライブ装置，ＤＶＤ－ＲＯＭドライブ装置，ＤＶＤ－ＲＡＭドライブ装置、フロッピーディスクドライブ装置（ＦＤＤ）等である。本実施形態では、実行形式のゲームプログラムが上記記録媒体に記録されて販売されている。

【００５１】通信装置４０７は、後述するユーザ登録時の登録キー、ユーザ固有データ等の各種データのサーバへの送信や、サーバからの認証データの受信を制御するものであり、例えばモデムやＬＡＮカード等である。

【００５２】音声出力装置４０２は、ゲームプログラムの音声データを出力するものでありスピーカ等である。表示装置４０３は、ゲームプログラムの画像データや、ユーザ登録プログラムで使用される各種データを表示するものでありディスプレイ装置が該当する。尚、表示装置４０３はテレビのディスプレイ装置に接続したものを用いても良い。

【００５３】入力装置４０４は、ゲームプログラムへの各種データや不正使用防止プログラムの各種データの入力を行うものであり、コントローラ、ジョイスティック、キーボード、マウス等である。

【００５４】（サーバのハードウェア構成）次に、サーバのハードウェア構成について説明する。図４に示すように、サーバには、制御装置４１１と、記憶装置４１５と、記録装置４１６と、通信装置４１７と、表示装置４１３と、入力装置４１４が接続されており、通常のコンピュータの構成となっている。

【００５５】制御装置４１１は、本実施形態のサーバ側で実行されるユーザ登録プログラムの動作を制御するＣＰＵ等の演算処理部と、ＲＯＭ等で構成されている。記憶装置４１５はメモリ等の一般的なＲＡＭで構成される。

【００５６】記録装置４１６は、ハードディスク（ＨＤ）等の不揮発性の記憶媒体、及びハードディスク（ＨＤ）へのリード／ライトを制御するハードディスクドライブ装置（ＨＤＤ）等である。本実施形態では、この記録装置４１６（ハードディスク）にユーザデータベース（ユーザＤＢ）４１８が格納されている。

【００５７】通信装置４１７は、ユーザ登録時の後述する登録キー、ユーザ固有データ等の各種データのゲーム装置からの受信や、ゲーム装置への認証データの送信を制御するものであり、例えばモデムやＬＡＮカード等である。

【００５８】表示装置４１３は、各種データを表示するものでありディスプレイ装置が該当する。また、入力装置４１４は、システム管理者等のサーバ使用者が各種データの入力を行うものであり、キーボード、マウス等である。

【００５９】（ゲーム装置の機能的構成）次に本実施形態に係るゲーム装置の機能的構成について説明する。本実施形態では、ゲームソフトウェアはゲームプログラムをＣＤ－ＲＯＭ、又はＤＶＤ－ＲＯＭ等の記録媒体に記録してパッケージとして提供される。各記録媒体には、予め所定の記憶領域に記録媒体に固有のシリアル番号が格納されており、シリアル番号は販売されるソフトウェアパッケージごとに異なるものとなっている。ゲームプログラムには、最初の起動時に実行されるユーザ登録プログラムと、２回目以降の起動時に実行されるユーザ認証プログラムと、ゲーム本体プログラムとから主に構成

されている。

【００６０】尚、ゲームプログラムをネットワーク経由でダウンロードする形式で提供するように構成しても良く、更に、ゲームプログラムや各種データの更新もネットワーク経由でダウンロードすることにより行うように構成することもできる。

【００６１】図５は、本実施形態に係るゲーム装置の機能的構成を示す機能ブロック図である。図５に示すように、本実施形態に係るゲーム装置は、起動部５０１と、ユーザ登録部５０２と、入力処理部５０４と、認証部５０３と、ゲーム本体部５０８とを備えたソフトウェア構成となっている。具体的には上記記録媒体に記録されたゲームプログラムをゲーム装置で起動することにより、起動プログラム、ユーザ登録プログラム、ユーザ認証プログラム、ゲーム本体プログラム、入力処理プログラムが記憶装置４０５（メモリ）上にロードされ、それぞれ起動部５０１、ユーザ登録部５０２、認証部５０３、ゲーム本体部５０８、入力処理部５０４が記憶装置４０５上に生成されるようになっている。ユーザ登録部５０２は、更に登録キー生成部５０５と、送受信処理部５０６と、セーブデータ生成部５０７とを備えている。

【００６２】起動部５０１は、ゲームプログラムを実行したときに、１回目の起動か、２回目の起動かを判断し、１回目の起動のときにはユーザ登録部５０２を呼び出し、２回目以降の起動のときには認証部５０３を呼び出すようになっている。

【００６３】入力処理部５０４は、本発明の入力処理手段を構成するものであり、ユーザ登録プログラム実行時にユーザ固有データの入力を促し、ユーザから入力されたユーザ固有データを送受信処理部５０６へ受け渡す。また、入力処理部５０４はゲーム本体部５０８の実行時に各種データを入力するようになっている。

【００６４】登録キー生成部５０５は、本発明の登録キー生成手段を構成するものであり、記録媒体からシリアル番号を読み出し、またゲーム装置の識別データ記憶部４０８に格納されている装置固有の装置識別番号を読み出して、読み出したシリアル番号と装置識別番号とを結合してサーバ送信用の登録キーを生成するものである。図８は、登録キーのデータ構造図である。この登録キーはシリアル番号及び装置識別番号毎に異なるように生成される。生成された登録キーは送受信処理部５０６へ出力される。尚、本実施形態では登録キーとして、シリアル番号と装置識別番号とを結合したデータとしているが、更に他のデータを含めた構成としても良い。

【００６５】また、図９は、ユーザ固有データのデータ構造図である。図９に示すように、ユーザ固有データは、氏名、生年月日、性別、住所、電話番号、電子メールアドレスからなるデータである。尚、ユーザ固有データは、ゲームプログラムを使用するユーザを識別できる情報を有していればよく、図９に示すデータの中の一部

のデータを有するように構成する他、更に他のデータを含めても良い。

【００６６】送受信処理部５０６は、自動的にサーバのＩＰアドレスを指定して通信装置４０７によってインターネットを介してサーバへ接続し、登録キー生成部５０５で生成された登録キーとユーザ固有データをサーバへ送信するようになっている。また、送受信処理部５０６は、サーバのシステム管理者等からサーバで生成された認証データを受信する。その他、送受信処理部５０６は、ゲーム進行に必要なデータや、ゲームプログラムの更新プログラムや各種データを受信するように構成することは任意である。

【００６７】セーブデータ生成部５０７は、受信した認証データからセーブデータを生成する。図１０は、サーバから受信する認証データのデータ構造図である。図１０に示すように、認証データは、シリアル番号、登録キー、ユーザ固有データからなるデータである。また、図１１は、ゲーム装置側で生成されるセーブデータのデータ構造図である。図１１に示すように、セーブデータは、シリアル番号、登録キー、ユーザ固有データの各データを暗号化したデータで構成される。セーブデータ生成部５０７は、受信した認証データの中の各データに公知の暗号処理を施すことにより認証データを生成する。生成されたセーブデータはセーブデータ記憶部４０９に格納され、特にユーザが明示的に削除しない限り、ゲーム装置の電源がＯＦＦの状態でもセーブデータ記憶部４０９に保持された状態となっている。

【００６８】認証部５０３は、ゲームプログラム実行ごとに起動され、ゲームプログラムを実行するユーザが正規のユーザか否かを、識別データ記憶部４０８に格納されている装置識別番号と、セーブデータ記憶部４０９に記憶されているセーブデータとから認証を行うものである。

【００６９】ゲーム本体部５０８は、ゲームの進行を制御するものであり、認証部５０３から呼び出されるようになっている。

【００７０】（サーバの機能的構成）次にサーバの機能的構成について説明する。図６は、サーバの機能的構成を示すブロック図である。図６に示すように、サーバは制御部６０１と、送受信処理部６０６と、認証データ生成部６０２と、登録部６０３と、ユーザデータベース４１８（ユーザＤＢ）とから構成されている。

【００７１】制御部６０１は、サーバで実行されるユーザ登録処理全体の制御を行うものである。送受信処理部６０６は、クライアントであるゲーム装置のユーザからインターネットで接続したユーザが送信した登録キーとユーザ固有データを受信し、自動生成された認証データをユーザに送信するものである。

【００７２】この認証データは、前述したように、認証データはシリアル番号と登録キーとユーザ固有データと

からなり（図１０参照）、認証データ生成部６０２により生成される。認証データ生成部６０２は、ユーザから受信した登録キーからシリアル番号を抽出し、抽出したシリアル番号と受信した登録キー及びユーザ固有データとを結合して認証データを生成する。この認証データは、ゲームソフトウェアを使用するユーザを認証するためのデータであり、ユーザ固有のデータとなっている。

【００７３】ユーザデータベース４１８（ユーザＤＢ）は、ゲームソフトウェアのユーザを管理するデータベースであり、記録装置４１６（ハードディスク）に格納されている。図７はユーザデータベース４１８のデータ構造図である。このユーザデータベース４１８は、シリアル番号をキーとした索引編成ファイルであり、データベース４１８に登録されるレコードは、図７に示すように、シリアル番号と、登録キーと、ユーザの氏名、生年月日、性別、住所、電話番号、電子メールアドレスからなるユーザ固有データとから構成されている。そして、各レコードのシリアル番号フィールドには、既に出荷されたゲームソフトウェアのパッケージに対応したシリアル番号が予め登録されており、各レコードごと（即ち、各ゲーム装置ごと）に異なる番号となっている。

【００７４】登録部６０３は、ユーザから受信したシリアル番号と同一のシリアル番号を有するレコードに、同じく受信した登録キーとユーザ固有データをWRITEして登録するものである。

【００７５】（ゲームシステムのユーザ登録処理）次に、以上のように構成された本実施形態のゲームシステムによるユーザ登録処理について説明する。図１はゲーム装置側でゲームプログラムを起動したときに実行される起動部５０１による起動処理のフローチャートである。

【００７６】ユーザがゲームプログラムを起動すると、起動部５０１では、第１回目の起動か否かを判断する（ステップ１０１）。具体的には、第１回目の起動時に、記憶装置４０５に任意のフラグデータを記録する。起動部５０１では、このフラグデータの有無をチェックすることにより１回目の起動か否かを判断する。即ち、フラグデータが存在しない場合には第１回目の起動であり、存在する場合には２回目以降の起動と判断する。そして、１回目の起動と判断された場合には、以下のユーザ登録処理が実行される（ステップ１０２）。２回目以降の起動と判断された場合には後述するユーザ認証処理が実行され（ステップ１０３）、その後ゲーム本体部５０８によりゲーム処理が実行される（ステップ１０４）。

【００７７】図２（ａ）は、本実施形態のゲーム装置側のユーザ登録部５０２で実行されるユーザ登録処理のフローチャートであり、図２（ｂ）はサーバ側のユーザ登録処理のフローチャートである。まず、登録キー生成部５０５により記録媒体の所定の記憶領域に格納されているシリアル番号を読み出して取得する（ステップ２０１）。次いで、入力処理部５０４により表示装置４０３に図１２に示す、ユーザの氏名や住所、電話番号、電子メールアドレス等のユーザ固有データの入力を促す表示画面を表示する（ステップ２０２）。このとき、ステップ２０１で取得したシリアル番号を、図１２の表示画面のシリアル番号フィールドに表示する。そして、ユーザに対し、上記各情報を入力装置４０４から入力させる（ステップ２０３）。

【００７８】次いで、登録キー生成部５０５により、識別データ記憶部４０８に格納されている装置識別番号を読み出し、この装置識別番号とステップ２０１で取得したシリアル番号とを結合して図８に示す登録キーを生成する（ステップ２０５）。そして、送受信処理部５０６によってサーバに接続し生成された登録キーとステップ２０３で入力されたユーザ固有データをサーバに送信する（ステップ２０６）。

【００７９】サーバ側では、送受信処理部６０６によってユーザのゲーム装置からユーザ固有データと登録キーとを受信する（ステップ２１０）。そして、認証データ生成部６０２によって、受信した登録キーからシリアル番号を抽出し、このシリアル番号と受信した登録キーとユーザ固有データとを結合して、図１０に示す認証データを生成する（ステップ２１１）。そして、サーバ側の送受信処理部６０６によって、生成した認証データをユーザのゲーム装置へ送信する（ステップ２１２）。

【００８０】次いで、サーバ側では、登録部６０３によってシリアル番号をキーとしてユーザデータベース４１８（ユーザＤＢ）内のレコードを検索し、ユーザから受信したシリアル番号のレコードに、ユーザから同じく受信した登録キーと、ユーザ固有データと、登録キーから抽出したゲーム装置の装置識別番号を登録する（ステップ２１３）。このようなデータベース４１８への登録は登録キーを送信した全てのユーザに対して行う。これにより、ユーザ登録が行われることになる。このように本実施形態のサーバでは、シリアル番号ごとにユーザ固有データをデータベース４１８に記録するので、一つのソフトウェアに対して使用可能なユーザを制限することができる。

【００８１】ユーザ側のゲーム装置では、サーバから認証データを受信すると（ステップ２０７）、認証データからシリアル番号、登録キー及びユーザ固有データをそれぞれ抽出し、各データを公知の暗号処理によって暗号化し、暗号化した各データを結合することによって、図１１に示すセーブデータを生成する（ステップ２０８）。そして、生成したセーブデータを、セーブデータ記憶部４０９に格納する（ステップ２０９）。

【００８２】（ゲーム装置での認証処理）セーブデータ記憶部４０９に格納されたセーブデータは、ゲーム装置を使用する際の認証に使用される。図３は、ゲーム装置

側の認証部５０３で実行される認証処理のフローチャートである。前述した図１に示すように、ユーザがゲームプログラムを起動すると起動部５０１によって１回目の起動か否かが判断され（ステップ１０１）、２回目以降の起動の場合に以下の認証処理が実行される（ステップ１０３）。

【００８３】認証部５０３では、まず識別データ記憶部４０８から装置識別番号を読み出し（ステップ３０１）、次にセーブデータ記憶部４０９からセーブデータを読み出す（ステップ３０２）。読み出したセーブデータは暗号化されているため、セーブデータを復号して、復号化されたセーブデータから登録キーを抽出し（ステップ３０３）、更に抽出した登録キーから装置識別番号を抽出する（ステップ３０４）。

【００８４】次いで、識別データ記憶部４０８から読み出した装置識別番号とセーブデータから抽出した装置識別番号とを比較する（ステップ３０５）。そして、両装置識別番号が同一の場合には、起動したゲーム装置がゲームプログラムを最初に起動してサーバに登録した装置での正当な使用であると判断してゲーム本体部５０８を起動する（ステップ３０６）。一方、両装置識別番号が異なる場合にはゲームプログラムを起動したゲーム装置は、サーバに登録した装置での使用でない不正使用であると判断して、実行できない旨又は不正使用である旨のエラーメッセージを出力して（ステップ３０６）、ゲーム本体５０８の実行を中止する。

【００８５】このように本実施形態のゲームシステムでは、サーバで生成された認証データに基づいてセーブデータを生成し、このセーブデータの中の装置識別番号に基づいた認証処理によりプログラムの使用が不正か否かを判断しているので、第１回目にゲームプログラムを起動したゲーム装置以外の装置で、サーバから認証データを受信してセーブデータを保存した場合でも、その装置ではゲームプログラムを起動することができなくなり、ゲームプログラムを複数のゲーム装置で使用するという不正使用を防止することができる。

【００８６】また本実施形態のゲームシステムでは、ハードウェアとしてのゲーム装置のセーブデータ記憶部４０９にセーブデータを格納するだけで不正使用を防止することができるので、製造コストの低減が図られる。

【００８７】尚、本実施形態のゲームシステムでは、シリアル番号を記録媒体に記録してソフトウェアパッケージを出荷する形態としているが、記録媒体にはシリアル番号を記録せずに、シリアル番号が記載されたシートをソフトウェアパッケージに添付して出荷する形態としても良い。この場合には、第１回目のプログラム起動時に図２のステップ２０１で登録キー生成部によって記録媒体からシリアル番号を読み出す代わりに、入力処理部５０４によってゲーム装置の表示装置４０３にシリアル番号入力画面を表示し、ユーザに入力装置４０４からシリアル番号を入力させて、登録キー生成部を入力されたシリアル番号と装置識別番号から登録キーを生成するように構成する必要がある。

【００８８】また、本実施形態のゲーム装置では、セーブデータの中の装置識別番号に基づいて不正使用か否かの判断を行っているが、更にセーブデータの中のユーザ固有データ、例えば氏名等に基づいた認証処理を行っても良い。この場合には、第１回目のゲームプログラム起動時にサーバに登録したユーザ以外の使用者か否かを判断することができ、ユーザのなりすましによるプログラムの不正使用を防止することができる。尚、この場合、認証処理の開始時に、ユーザに対し例えば図１２の入力画面等を表示して、氏名等のユーザ固有データの入力を要求するように構成する必要がある。

【００８９】また、セーブデータの中のシリアル番号に基づいた認証処理を行っても良い。この場合には、生成されたセーブデータを格納したゲーム装置以外の装置でゲームプログラムを実行することができなくなり、ゲームプログラムを複数の装置で使用するという不正使用を防止することができる。シリアル番号に基づいた認証処理を行う場合には、本実施形態のゲームシステムのようにシリアル番号を予め記録媒体に記録して出荷している形態においては、認証処理の開始時に、シリアル番号を記録媒体から読み出す構成とする必要がある。また、シリアル番号を記録媒体には記録せずに、シリアル番号が記載されたシートをソフトウェアパッケージに添付して出荷する形態とする場合には、認証処理の開始時に、ユーザに対しシリアル番号の入力を要求するように構成する必要がある。

【００９０】本実施形態では、本発明をゲームシステムに適用しているが、登録ユーザに対してのみソフトウェアを実行させるシステムであれば任意のシステムに適用することが可能である。

【００９１】

【発明の効果】以上説明した通り、本発明によれば、一つのソフトウェアに対して使用可能なユーザを確定して制限することができるという効果を有する。また、記録媒体のプログラムを複数の装置で実行するという不正使用を防止できるという効果を有する。また、記録媒体の不正コピーが実質的に無効となり、不正コピーの抑止が図られるという効果を有する。更に、データ改竄によるプログラムの不正使用を防止できるという効果を有する。加えて、不正使用防止のためのハードウェアを特別に設ける必要がなく、製造コストの低減が図られるという効果を有する。

【００９２】また、本発明によれば、不正ユーザの正規ユーザのなりすましによるプログラムの不正使用を防止できるという効果を有する。

【図面の簡単な説明】

【図１】本実施形態のゲーム装置で実行される起動処理

のフローチャートである。

【図２】図２（ａ）は、本実施形態のゲーム装置で実行されるユーザ登録処理のフローチャートであり、図２（ｂ）は、本実施形態のサーバで実行されるユーザ登録処理のフローチャートである。

【図３】本実施形態のゲーム装置で実行されるユーザ認証処理のフローチャートである。

【図４】本実施形態のゲームシステムの全体構成を示すハードウェア構成図である。

【図５】本実施形態のゲーム装置のソフトウェア構成（機能的構成）を示すブロック図である。

【図６】本実施形態のサーバのソフトウェア構成（機能的構成）を示すブロック図である。

【図７】本実施形態のサーバの記録部に格納されたユーザデータベースの構造図である。

【図８】本実施形態のゲーム装置で生成される登録キーのデータ構造図である。

【図９】本実施形態のゲームシステムで使用されるユーザ固有データのデータ構造図である。

【図１０】本実施形態のサーバで生成される認証データのデータ構造図である。

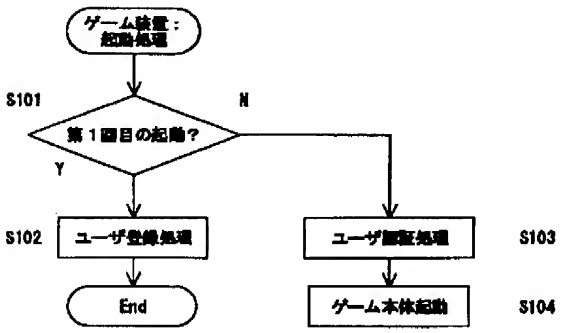
【図１１】本実施形態のゲーム装置で生成されるセーブデータのデータ構造図である。

【図１２】本実施形態のゲーム装置で表示されるユーザ固有データの入力画面の模式図である。

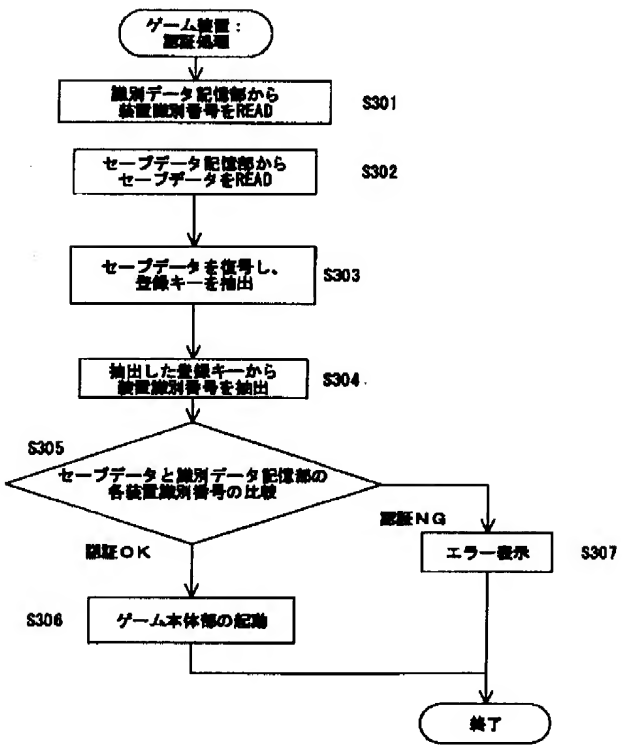
【符号の説明】

４０１、４１１：制御装置
４０２：音声出力装置
４０３、４１３：表示装置
４０４、４１４：入力装置
４０５、４１５：記憶装置
４０６：外部記憶装置
４０７、４１７：通信装置
４０８：識別データ記憶部
４０９：セーブデータ記憶部
４１６：記録装置
４１８：ユーザデータベース
５０１：起動部
５０２：ユーザ登録部
５０３：認証部
５０４：入力処理部
５０５：登録キー生成部
５０６：送受信処理部
５０７：セーブデータ生成部
５０８：ゲーム本体部
６０１：制御部
６０２：認証データ生成部
６０３：登録部
６０６：送受信処理部

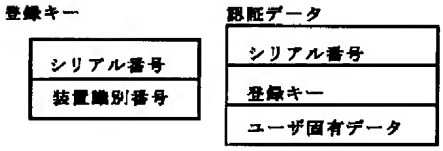
【図１】



【図３】

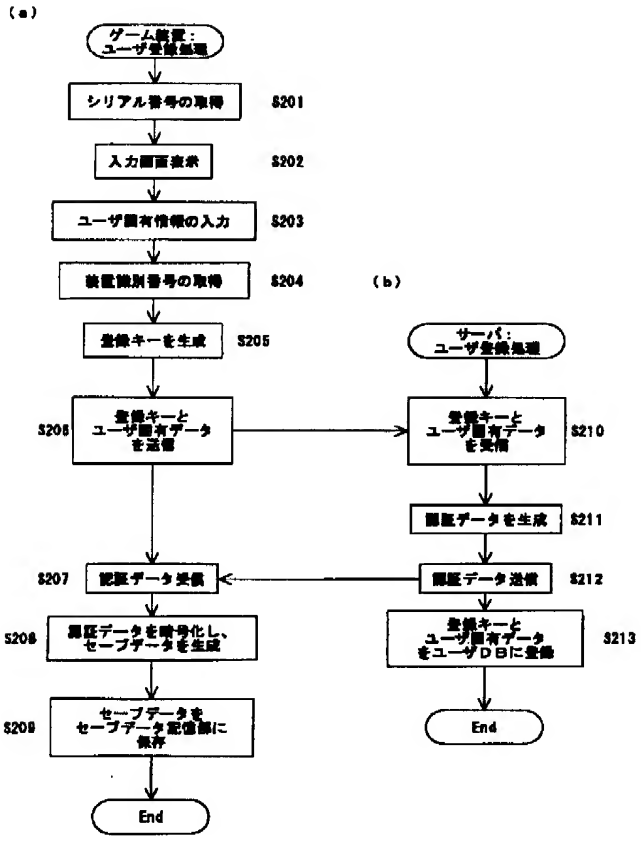


【図８】

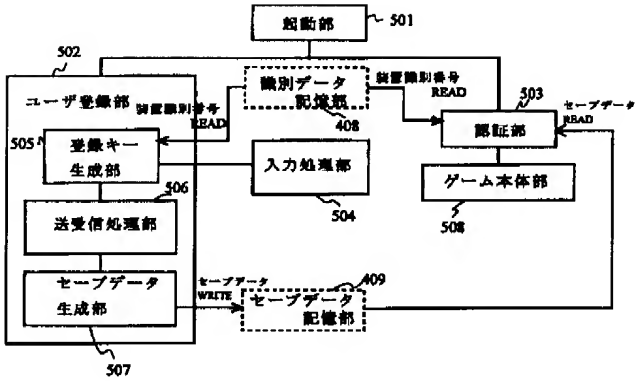


【図１０】

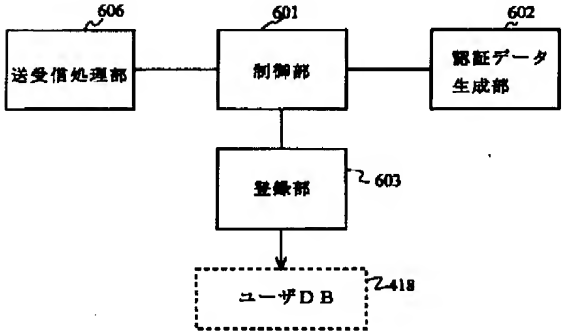
【図２】



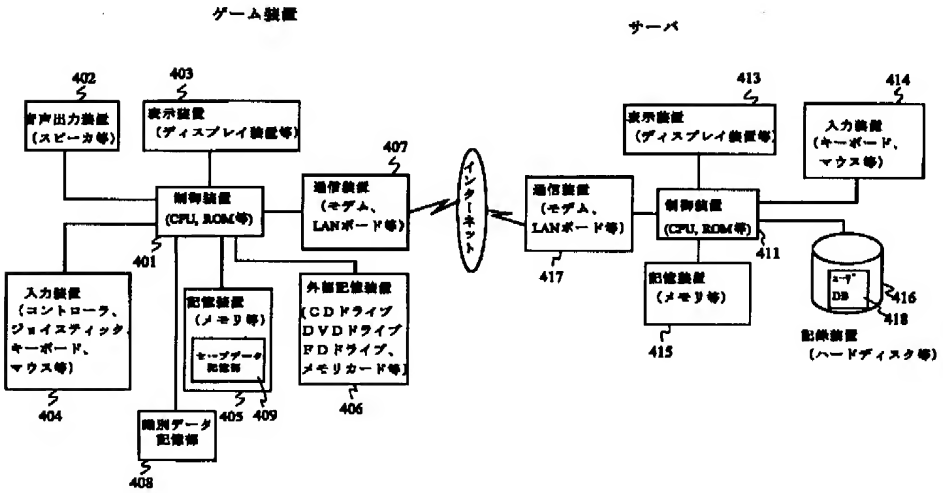
【図５】



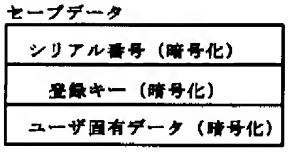
【図６】



【図４】



【図１１】



【図７】

ユーザＤＢ

シリアル番号	ユーザ固有情報	登録キー	装置識別番号
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・

【図９】

ユーザ固有データ

氏名
生年月日
性別
住所
電話番号
電子メールアドレス

【図１２】